15 апреля 2014

Как виртуализация может упростить вашу стратегию BYOD

Комментарий Андрея Мелузова, руководителя департамента ИТ-аутсорсинга "КОРУС Консалтинг", к статье портала Think Innovative о тенденциях в среде BYOD и виртуализации.

1. Все больше и больше компаний позволяет сотрудникам или поощряет их приносить свои мобильные устройства (BYOD) на работу. Ожидается, что эта тенденция в ближайшие годы станет распространенным явлением. Насколько распространена в российской практике внедрения BYOD виртуализация приложений, когда администраторы публикуют приложения в частном облаке, разрешая пользователям соединяться с ним через безопасный портал HTTPS?

На самом деле, практика развертывания приложений для доступа с персональных устройств сотрудников пока еще не очень распространена. Администраторы и бизнес только приходят к пониманию такой необходимости. Мы все понимаем основные риски: на персональном ноутбуке сотрудника может быть не установлено ни антивирусов, ни Firewall, могут быть установлены вредоносные программы и вирусы. И сейчас у администраторов нет единой концепции, как с этим бороться. Одним из

путей решения является использование приложений, ориентированных на BYOD, которые разворачиваются в так называемом DMZ (Демилитаризованная зона - часть сети, которая изолирована от основной сети: даже если произойдет заражение машины в этой зоне – основная сеть останется невредимой).

Но на мой взгляд, покупка сервиса напрямую – более правильное решение. Когда у пользователей, администраторов просто нет доступа к уровню администрирования, глубинному уровню операционной системы приложения и, соответственно, нет необходимости поддерживать данный сервис. В таком случае, если даже персональный компьютер сотрудник будет напичкан вирусами, то в случае использования приложения у вируса просто не будет возможности прописаться в операционной системе. Этот вариант гораздо более безопасен , чем когда мы допускаем пользователя со своим устройством в приложение, развернутое на нашем сервере. Таким образом, HTTPS-трафик застрахует нас от потери информации по пути от персонального компьютера до приложения, а использование сервиса страхует нас от вредоносного контента в этом трафике.

2. Какие плюсы заключает в себе этот аспект BYOD?

Самым большим плюсом я считаю минимизацию риска перехвата информации. Среди минусов: в случае собственной виртуализации остается доступ к операционной системе.

3. Как разные технологии виртуализации могут облегчить работу концепции BYOD на предприятии? Какие именно

технологии виртуализации применяются чаще?

Признаться, я не вижу особой связи между технологиями визуализации и концепцией BYOD. Безусловно, технологии виртуализации помогают минимизировать риски, связанные с надежностью решений, но они не влияют на работоспособность приложения. Если мы говорим не только о технологиях виртуализации, а о сервисах в целом – о том, что нам может помочь для управления всем набором разнообразных приложений – то здесь список тем для обсуждения расширяется. Появились новые облачные сервисы для управления устройствами (например, Microsoft Intune), сервисы, позволяющие осуществлять мониторинг вирусной активности, удаленно настраивать антивирусы, параметры безопасности и подключать персональные устройства к сервисам. Также концепция BYOD нашла распространение в сетевых мониторах, сетевых сервисах, которые проверяют трафик с персональных устройств и, в случае обнаружения вирусов, ставит устройства на карантин.

http://thinkinnovative.ru/materials/analytics/id/1623#expert_opinion_15